IT Policy

Introduction

This policy covers the security and use of The UK College of English's information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all UKCE employees, contractors, students and agents (hereafter referred to as "individuals").

Scope

This policy applies to all information, in whatever form relating the UKCE's business activities worldwide, and to all information handled by UKCE relating to other organisations and individuals with whom it deals. It also covers all IT and information communication facilities operated by UKCE or on its behalf. IT defines a framework of which UKCE's computer systems, assets, infrastructure and computing environment will be protected from threats whether internal, external, deliberate or accidental.

Individual's Responsibility

Access to the UKCE's IT systems are controlled by the use of the User ID's and passwords. All User ID's and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the UKCE IT systems.

In order to reduce the risk of unauthorised access or loss of information, individuals must:

- Comply with current legislation and legal requirements;
- Use College Computer Workstations, internet access and UKCE's email system in an acceptable manner;
- Protect individuals' personal or confidential business information
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended;
- Care must be taken to not leave confidential material on printers or photocopiers;
- User names and passwords must not be shared with other individuals or left unattended.

Individuals must NOT:

- Use the internet or email for the purposes of harassment or abuse
- visiting sites on the internet that contain, obscene, hateful, pornographic, anything considered as an extremist site or activity, sites considered to encourage radicalisation or sites considered damaging to the College's systems
- using the internet to send offensive or harmful material to others
- using the internet to access sites delivering streaming facilities whether they are audio or visual
- downloading any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence in place between UK College of Business and Computing and a third party

- downloading any non-commercial shareware, freeware or open source software without prior written permission from the network administrator at UK College of Business.
- downloading any web browser toolbars or search assistants without prior written permission from the network administrator
- hacking into unauthorised areas
- transmitting defamatory materials
- allow other individuals to use their User ID or Passwords on any IT system
- leave there user accounts logged in at an unattended and unlocked computer
- use another individuals User ID and Password to access UKCE's IT systems
- leave their password unprotected (for example by writing it down)
- causing unruly or threatening behaviour is not acceptable and is considered a serious offence
- perform any unauthorised changes to the UKCE's IT system or information
- attempt to access data that they are not authorised to use or access
- exceed the limits on their authorisation or specific business need to interrogate the system or data
- connect any non-authorised devices to the network or IT system
- visiting Internet sites that contain obscene, hateful, offensive, harassing, pornographic material, extremist propaganda or any sites relating to it
- introducing any form of computer virus into the corporate network
- store personal files such as music, video, photographs or games on IT equipment;
- remove or disable anti-virus software
- attempt to remove virus-infected files or clean up an infection, other than by the use of approved anti-virus software and procedures by authorised staff – network administrator at UKCBC
- broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- to perpetrate any form of fraud, encourage "radicalisation" or software of music piracy;

Monitoring

Individuals that have access to personal data (as defined under the Data Protection Act 1998) are responsible for ensuring that such data is not made available to unauthorised and that the security of all systems used to access and manage this data is not compromised.

Any portable equipment (such as laptops, portable telephones, memory sticks,) should be stored in a safe and secure location when not in use.

- All breaches of security must be reported immediately to the network administrator at UKCBC as they may be further implications to the I.T. security systems.
- The College has the right to access the personal account after the "individual" member leaves its employment and for the continuing delivery of services.
- All individuals should be aware that the College conducts random monitoring of communications, regardless of whether the use is business or personal.

The College reserves the right for appropriate authorised staff to examine any data including personal data held on its systems when operationally necessary. The network administrator or identified and authorised members of staff are permitted to examine data within individual accounts and network traffic, but will only do so when operationally necessary.

Monitoring may involve:

- Examining the number and frequency of emails;
- Examining the number and frequency of telephone calls;
- Viewing sent or received emails from a particular source;
- Examining logs of ICT facility usage;
- Monitoring the amount of time spent on the Internet;
- Internet sites visited and information downloaded.

Sanctions

IT systems logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. This will be carried out by the IT department at UK College of Business and Computing. UKCBC has the right (under certain conditions) to monitor activity on its systems, including the internet and email use, in order to ensure systems security, effective operation, protect individuals against misuse or threats from propaganda and extremism. UKCBC also operates a filtering system whereby certain websites are not accessible i.e. advertising or any sites that are deemed in appropriate, the aim is to protect the welfare of its community.

We consider it unacceptable for our IT networks to be used in any way that supports, promotes or facilitates terrorism. The use of IT has been referenced in our Safeguarding and Prevent Policies and is under constant review. Other means of communications such as social media, i.e. Facebook, Instagram have been highlighted as a possible means for potential extremist propaganda to by-pass systems. At UKCE our IT services are monitored on a regular basis by the IT department at UKCBC using specific filtering software, which limits access to harmful content such as pornographic, propaganda, extremist, radicalisation, or any sites deemed as inappropriate.

Where it is believed that the individual has failed to comply with this policy, they will face the College's disciplinary procedures. If the individual is found to have breached this policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. Any breaches in any of the above could result in disciplinary action taken against employees as discussed in staff handbook. Any employee or student found to be accessing any information regarded as promoting extremist views, propaganda etc could face expulsion from the college and police prosecution.

- Evidence will be provided showing how individuals have failed to comply with the Information Technology (IT) Policy. Individuals will then be asked to explain their reasons for failing to comply. Should the reasons provided prove to be unsatisfactory a first written warning will be issued. Students will also have to sign a code of conduct.
- Evidence will be provided showing how individuals have failed to comply with the Information Technology (IT) Policy. Employees will then be asked to explain their reasons for failing to comply.

Should the reasons provided prove to be unsatisfactory a second and final written warning will be issued.

- If the individual/s choose to ignore a final written warning and once more fail to comply with these guidelines, full disciplinary action will be taken which will constitute as gross misconduct on the part of the individual.

Roles and Responsibilities

All individuals should familiarise themselves of the College's responsibilities with regard to its Information Technology (IT) Policy and abide by is content.

Reviewed in December 2019

Reviewed annually or more often if required